UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

Anthony Grippa, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. BetMGM, LLC Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Anthony Grippa, ("Plaintiff"), individually and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant BetMGM, LLC ("Defendant" or "BetMGM") and allege, upon personal knowledge as to his own actions and upon information and belief, including his counsels' investigations, as to all other matters, as follows:

I. NATURE AND SUMMARY OF THE ACTION

1. This action stems from Defendant's failure to secure the sensitive personal information of their current and former customers, and other consumers for whom Defendant performed services.

2. BetMGM is the exclusive sports betting division of MGM Resorts International ("MGM"), both online and in MGM casinos nationwide.

3. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive personally identifiable information provided by and belonging to their customers, including, without limitation, name, email address, postal address, phone number, date of birth, hashed Social Security number, account identifier, and information related to transactions (collectively, "PII").

4. It is believed that sometime in May 2022, a third party actor gained entry to Defendant's network systems, accessed the PII stored therein, and exfiltrated information (the "Data Breach").

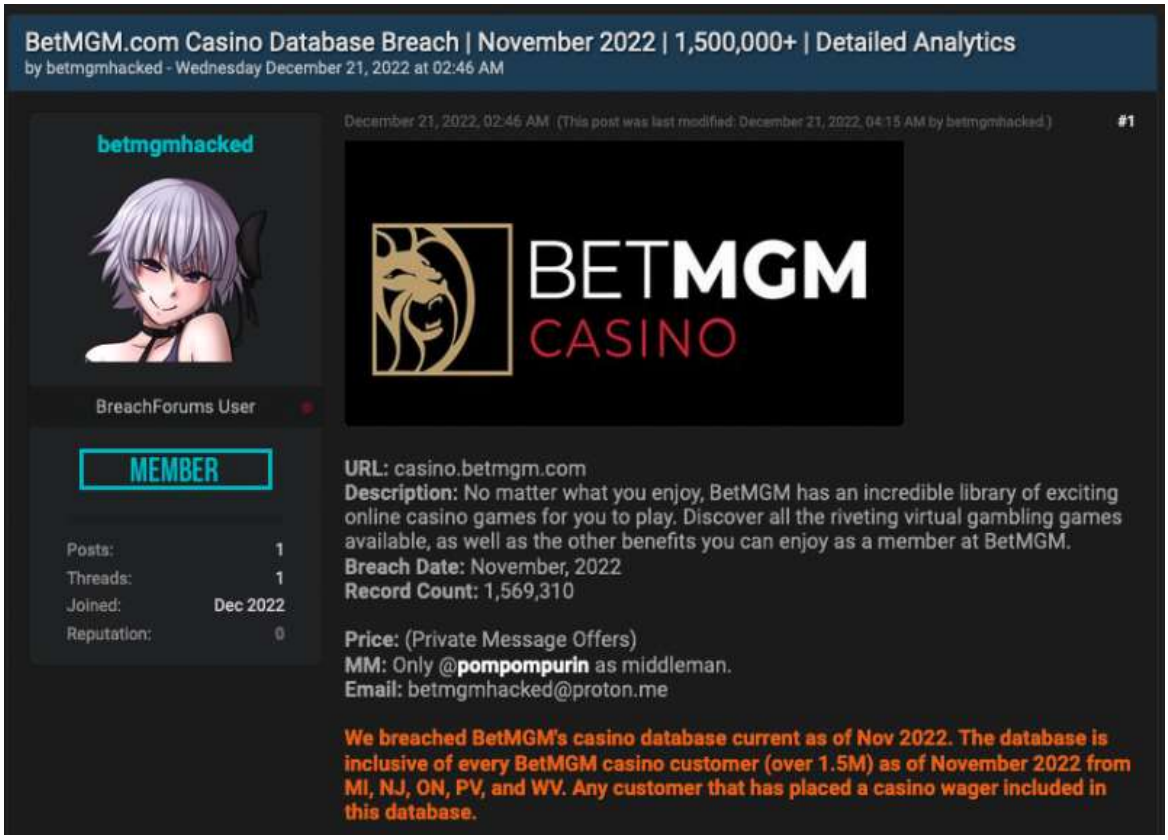
5. It is believed that the PII of any customer that placed a casino wager using BetMGM was unlawfully acquired by a third party actor.

6. On December 21, 2022, Defendant, through its website, announced that its security had been breached.[1]

7. Defendant stated that it first learned of the Data Breach on November 28, 2022, and that it had no evidence that patron passwords or account funds were accessed.

8. It is unknown what spurred Defendant to announce that its security had been breached, considering that it had been sitting on the information for nearly a month.

9. It may be coincidental, but on December 21, 2022, at 2:46 a.m., an unknown third party actor advertised that the PII obtained through the Data Breach was being advertised for sale on a popular cybercrime forum.[2]



[1] *BetMGM Notice,* available at: https://www.betmgminc.com/notice-regarding-patron-personal-information/
[2] *BetMGM Confirms Breach as Hackers Offer to Sell Data of 1.5 Million Customers*, Security Week (December 2022), available at: https://www.securityweek.com/betmgm-confirms-breach-hackers-offer-sell-data-15-million-customers

10. Defendant's delayed response adversely affected Plaintiff and other class members as they could have undertaken proactive measures to secure their PII. Instead, Defendant sat on this important information to the detriment of Plaintiff and the Class, until Defendant's hand was forced by the cybercrime posting.

11. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class members; (ii) warn Plaintiff and Class members of their inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities. Defendant's conduct amounts to at least negligence and violates federal and state statutes designed to prevent or mitigate this very harm.

12. Plaintiff and Class Members have suffered actual and present injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft for their respective lifetimes; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the present and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (f) damages to and diminution in value of their personal data entrusted to Defendant on the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (g) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' PII.

Plaintiff and Class Members, at the very least, are entitled to damages and injunctive relief tailored to address the vulnerabilities exploited in the breach, and designed to protect Plaintiff and Class Members' PII, as well as an order directing the destruction and deletion of all PII for which Defendant cannot demonstrate a reasonable and legitimate purpose for continuing to maintain possession of such PII.

13. Defendant understands the need to protect the privacy of their customers and use security measures to protect their customers' information from unauthorized disclosure. And as sophisticated financial entities who maintain private and sensitive consumer information, Defendant and its corporate affiliates further understood the importance of safeguarding PII.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

15. As a result of Defendant's actions, the PII of Plaintiff and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

16. Plaintiff by this action seeks compensatory damages together with injunctive relief to remediate Defendant's failures to secure their and the other Class Members' PII, and to provide damages, among other things, for Plaintiff and Class Members to secure identity theft insurance,

and credit repair services for Class Members' respective lifetimes to protect the Class of Data Breach victims from identity theft and fraud.

II. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

18. Venue is proper under 18 U.S.C § 1391(b)(1) in this Judicial District as substantial acts and part of the events or omissions giving rise to the claims as alleged in this Class Action Complaint occurred in this District.

19. The District of New Jersey has personal jurisdiction over Defendant because Defendant is a corporation of New Jersey with a principal place of business in this District.

III. PARTIES

20. Plaintiff Anthony Grippa, is a current MGM customer.

21. Plaintiff Grippa is a citizen and resident of the Commonwealth of Pennsylvania, currently residing in Pittsburgh. Plaintiff Grippa learned of the Data Breach because of a notice letter sent by Defendant, dated December 21, 2022.

22. Defendant BetMGM, LLC is incorporated under the laws of the State of New Jersey, with its principal office located at 210 Hudson Street, Jersey City, New Jersey 07302.

IV. FACTUAL ALLEGATIONS

23. Defendant BetMGM is the exclusive sports betting division of MGM, both online and in MGM casinos nationwide.

24. BetMGM is also the headline brand for online casino gaming alongside sister brands Borgata Online, Party Casino and Party Poker.

25. In order to engage with BetMGM's business, Plaintiff and Class Members were required to provide their PII, including names, dates of birth, and social security numbers, among other sensitive information.

26. Defendant possessed the PII of Plaintiff and Class Members within its computer systems.

27. Defendant implicitly and/or explicitly represented to Plaintiff and Class Members, that their PII would be secured.[3]

28. Defendant had duties and obligations through common law, federal regulations, contracts, industry standards, and their representations to Plaintiff and Class Members that Defendant would adopt reasonable measures to protect the PII of Plaintiff and Class Members from third party actors.

The Data Breach

29. On December 21, 2022, Defendant announced for the first time that it had been subject to the Data Breach.

30. Earlier that same day, a third party actor posted to a cybercrime forum that it had breached Defendant's cyber security, and that the PII of Plaintiff and Class Members were for sale.

[3] *BetMGM Privacy Policy*, available at: https://sports.betmgm.com/en/blog/privacy-policy

31. Later that day, Defendant began notifying Plaintiff and Class Members that their data had been stolen, informing them of the following:

> We are writing to notify you of an issue that involves certain of your personal information. We have learned that certain BetMGM patron records were obtained in an unauthorized manner. We believe that your information was contained in these records, which may have included details such as name, contact information (such as postal address, email address and telephone number), date of birth, hashed Social Security number, account identifiers (such as player ID and screen name) and information related to your transactions with us. The affected information varied by patron.
>
> We promptly launched an investigation after learning of the matter and have been working with leading security experts to determine the nature and scope of the issue. We learned of the issue on November 28, 2022, and believe the issue occurred in May 2022. We currently have no evidence that patron passwords or account funds were accessed in connection with this issue. Our online operations were not compromised. We are coordinating with law enforcement and taking steps to further enhance our security.
>
> We recommend you remain alert for any unsolicited communications regarding your personal information and review your accounts for suspicious activity. We take our obligation to safeguard personal information very seriously and have arranged to offer you credit monitoring and identity restoration services for two years at no cost to you. The Reference Guide below provides instructions on enrolling in these services and steps you can take to protect your information.[4]

32. This data breach letter failed to explain why Defendant was unable to detect the Data Breach for six months, the remedial measures undertaken once knowledge of the breach occurred, and why Defendant did not notify Plaintiff and Class Members in a timely manner once Defendant discovered the breach.

[4] Exhibit A. Data Breach Letter.

The Value of Personally Identifiable Information (PII)

33. PII is very valuable to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information is sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[5]

34. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[6]

35. Social Security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

36. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of

---

[5] *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on- the-dark-web-how-much-it-costs/

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your- personal-information-is-selling-for-on-the-dark-web/

[7] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.

37. Even then, a new Social Security number may not be effective. According to the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[8]

38. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, in that situation, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, financial history, and Social Security number.

39. This data commands a much higher price on the black market. "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[9]

40. Identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police, among other forms of fraud.

41. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

[8] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s- hackers-has-millionsworrying-about-identity-theft

[9] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

42. Further, there may be a time lag between when harm occurs and when it is discovered and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

43. Plaintiff and Class Members now face a lifetime of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damage in addition to any fraudulent use of their PII.

Gambling Companies are Targeted by Cybercriminals

44. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on their network, comprising millions of individuals' detailed and confidential personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

45. Data thieves regularly target companies like Defendant's due to the large volumes of PII that they come into possession of.

46. As custodians of Plaintiff and Class Member's PII, Defendant knew or should have known the importance of protecting their PII, and of the foreseeable consequences if any data breaches occurred.

47. Defendant's security obligations were especially important due to the substantial up-tick of cyber-attacks and data breaches occurring in recent years.

[10] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf

48. Furthermore, Defendant should have been vigilant in protecting its data as gambling companies such as Defendant, are especially targeted for cyber-attacks.

2014, Las Vegas Sands Data Breach.[11]
2020, BetAmerica, Golden Nugget, Resorts, SDTech cyberattack.[12]
2020, Clubillion Data Breach[13]
2021, Golden Entertainment Data Breach[14]

49. Furthermore, it is inconceivable that BetMGM would not know of its danger to data breaches, considering that its parent operator, MGM Resorts suffered from a data breach in 2019, whereby 10.6 million people's PII was stolen.[15]

Common Injuries and Damages to Plaintiff and Class Members

50. Although Defendant have offered identity monitoring services for a limited time, the offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the highly sensitive nature of the PII at issue here.

51. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures to protect the PII of BetMGM's current and former customers.

52. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members are presently experiencing and will continue experiencing actual harm from fraud and identity theft.

---

[11] *Iran hacked an American Casino, U.S. says,* (February 27, 2015), CNN, *available at:* https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html

[12] *Some US Online Gambling Sites Down Following Cyberattack on SBTech*, (March 30, 2020) Legal Sports Report, *available at*: https://www.legalsportsreport.com/39533/sbtech-cyber-attack/

[13] Casino App Clubillion Leaks PII on "Millions of Users", Infosecurity Group (July 8, 2020), available at: https://www.infosecurity-magazine.com/news/casino-app-clubillion-leaks-pii/

[14] Golden Entertainment Phishing Attack Leads to Personal Information Being Exposed, Id Theft Center (February 18, 2020), available at: https://www.idtheftcenter.org/post/golden-entertainment-phishing-attack-leads-to-personal-information-being-exposed/

[15] MGM Resorts sued over data breach that possibly involved 10.6 million guests, Reuters, (February 22, 2020), available at: https://www.reuters.com/article/us-mgm-resorts-intl-cyber-lawsuit-idUKKCN20G062

53. Plaintiff and Class Members are presently experiencing substantial risk of out-of-pocket fraud losses, such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

54. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

55. Plaintiff and Class Members are also incurring and may continue incurring out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

56. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by the cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

57. Plaintiff and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;
b. Purchasing credit monitoring and identity theft prevention;
c. Placing ‘freezes’ and ‘alerts’ with credit reporting agencies;
d. Spending time with financial institution or government agencies to dispute fraudulent charges and/or claims;
e. Contacting financial institutions and closing or modifying financial accounts; and
f. Closely reviewing and monitoring Social Security number, bank accounts, payment card statements, and credit reports for unauthorized activity for years to come.

58. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by

the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

59. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

60. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a substantial and present risk of harm.

IV. CLASS ACTION ALLEGATIONS

61. Plaintiff brings this action as a class action pursuant to Rule 23 *et seq.* of the Federal Rules of Civil Procedure on behalf of the Class.

62. Plaintiff propose the following Class Definition:

> **All individuals whose PII was compromised in the Data Breach as described in Defendant's notice to Plaintiff and Class Members.**

63. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, members, affiliates, officers and directors, and any entity in which a Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

64. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

65. The members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court.

66. Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These questions include but are not limited to:

a. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

b. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices adequate to protect the information compromised in the Data Breach, considering its nature and scope;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Defendant violated state statutes as alleged herein;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiff and Class Members;

i. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

67. Plaintiff's claims are typical of those of the Class because Plaintiff and the Class sustained damages from Defendant's wrongful conduct.

68. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff will fairly and adequately represent and protect the interests of the Class Members. No Plaintiff has a disabling conflict of interest with any other Member of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class, and the infringement of rights and the damages they have suffered are typical of other Class Members. Plaintiff also has retained counsel experienced in complex class action litigation, and they intend to prosecute this action vigorously.

69. As provided under Fed. R. Civ. P. 23(b)(2), Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct in relation to the Class and making final injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff challenges these policies by reference to Defendant's conduct with respect to the Class as a whole.

70. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation makes it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

71. Consistent with Fed. R. Civ. P. 23(b)(3), class treatment is superior to all other available methods for the fair and efficient adjudication of this controversy. Among other things, it will permit a large number of Class Members to prosecute their common claims in a single

forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Moreover, class action treatment will permit the adjudication of relatively modest claims by Class Members who could not individually afford to litigate a complex claim against large corporations such as Defendant. Prosecuting the claims pleaded herein as a class action will eliminate the possibility of repetitive litigation. There will be no material difficulty in the management of this action as a class action.

72. Particular issues, such as questions related to Defendant's liability, are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the resolution of such common issues would materially advance the resolution of this matter and the parties' interests therein.

73. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. Prosecution of separate actions by Class Members also would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class Against Defendant)

74. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

75. Plaintiff brings this claim on behalf of himself and the Class.

76. As a condition of using the service of Defendant or its partners or affiliates, Plaintiff and the Class were required to provide and entrust Defendant with certain PII, including their name, birthdate, address, loan number, Social Security number, and other information.

77. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

78. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their systems and networks—and Plaintiff and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

79. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

80. Defendant knew or reasonably should have known that its failure to exercise due care in the collecting, storing, and using of consumers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

81. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and Class Members' information in their possession was adequately secured and protected.

82. Defendant also had a duty to exercise appropriate practices to remove former customers' PII that they were no longer required to retain pursuant to regulations.

83. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

84. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in receiving services from Defendant. While this special relationship exists independent from any contract, it is recognized by Defendant's Privacy Policies, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered PII as part of its business and was solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class members from a resulting data breach.

85. Defendant was subject to an independent duty, untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

86. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

87. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems. It was foreseeable that Plaintiff and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

88. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included

their decision not to comply with industry standards for the safekeeping of Plaintiff and the Class's PII, including basic encryption techniques available to Defendant.

89. Plaintiff and the Class had and have no ability to protect their PII that was in, and remains in, Defendant's possession.

90. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

91. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

92. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

93. Defendant, through its actions and inaction, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

94. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

95. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

96. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former customers' PII.

97. Defendant, by its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

98. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

99. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff and the Class's PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

100. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

101. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

102. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

103. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

104. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

105. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former customers' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

106. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

107. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

108. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

109. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant)

110. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

111. Plaintiff bring this claim on behalf of himself and the Class.

112. Defendant acquired and maintained the PII of Plaintiff and the Class, including names, birthdates, addresses, loan numbers, Social Security numbers, and information provided in connection with Defendant's business.

113. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

114. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would not properly secure the PII, and not delete the PII that Defendant no longer had a reasonable need to maintain.

115. Defendant further implicitly promised to comply with industry standards and to ensure that Plaintiff and the Class Members' PII would remain protected.

116. Implicit in the agreements between Plaintiff and the Class and Defendant to provide PII, was the latter's obligation to:

a. Use such PII for business purposes only;

b. Take reasonable steps to safeguard the PII;

c. Prevent unauthorized disclosures of the PII;

d. Provide Plaintiff and the Class with prompt and sufficient notice of any and all unauthorized disclosure or uses; and

e. Retain the PII only under conditions that kept such information secure and confidential.

117. In collecting and maintaining the PII of Plaintiff and the Class and publishing its privacy policies, Defendant entered into implied contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiff and the Class.

118. Plaintiff and the Class fully performed their obligations as required with Defendant.

119. Defendant breached the implied contract it made with Plaintiff and the Class by failing to protect and keep private the financial information of Plaintiff and the Class, including failing to;

a. Encrypt or tokenize the sensitive PII of Plaintiff and the Class;
b. Delete such PII that Defendant no longer had reason to maintain;
c. Eliminate the potential accessibility of the PII where such accessibility was not justified; and
d. Otherwise review and improve the security of the network system that contained such PII.

120. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer): ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity

theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

121. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class are at an increased risk of identity theft or fraud.

122. As a direct and proximate result of Defendant's breach of implied contracts, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class Against Defendant)

123. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

124. Plaintiff bring this claim on behalf of himself and the Class.

125. A relationship existed between Defendant and Plaintiff and the Class in which Plaintiff and the Class put their trust in Defendant to protect the PII of Plaintiff and the Class and Defendant accepted that trust.

126. Defendant breached the fiduciary duty that they owed to Plaintiff and the Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the Class.

127. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

128. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

129. Lakeview's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Class.

130. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT IV
VIOLATION OF STATE STATUTES
(On Behalf of Plaintiff and the Class Against Defendant)

131. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

132. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or manages computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was unlawfully acquired by an unauthorized person. These statutes also require that the disclosure of the breach be made in the most expedited time possible and without unreasonable delay.

133. Defendant's Data Breach is covered under the meaning of the below mentioned state data breach statutes, and the data that was unlawfully acquired was protected and covered by the below data breach statutes.

134. Plaintiff and Class Members' PII constitute personal information as covered under the state data breach statutes, and any loss of such PII is governed by the state data breach statutes.

135. Defendant failed to timely notify and disclose the Data Breach to affected customers, including Plaintiff and the Class.

136. As a direct and proximate result of Defendant's failure to notify Plaintiff and the Class, as required by the below state data breach statutes, Plaintiff and the Class were injured. Had Defendant provided timely and accurate notice of the Data Breach, Plaintiff and the Class could

have mitigated any injuries that may have arose from Defendant's unreasonable delay to provide notice.

137. Defendant's failure to protect Plaintiff and the Class's PII and subsequent failure to timely notify Plaintiff and the Class of the Data Breach, violated the following state data breach statutes (including any revisions, modifications, and additions):

a. Alaska Stat. § 45.48.010(a), et seq.;

b. Ark. Code § 4-110-105(a), et seq.;

c. Cal. Civ. Code § 1798.83(a), et seq.;

d. Colo. Rev. Stat. § 6-1-716(2), et seq.;

e. Conn. Gen. Stat. § 36a-701b(b), et seq.;

f. Del. Code Tit. 6 § 12B-102(a), et seq.;

g. D.C. Code § 28-3852(a), et seq.;

h. Fla. Stat. § 501.171 (4), et seq.;

i. Ga. Code § 10-1-912(a), et seq.;

j. Haw. Rev. Stat. § 487N-2(a), et seq.;

k. Idaho Code § 28-51-105(a), et seq.;

l. 815 ILCS 530/1, et seq.;

m. Iowa Code § 715C.2(1), et seq.;

n. Kan. Stat.§ 50-7a02(a), et seq.;

o. Ky. Rev. Stat. § 365. 735(2), et seq.;

p. La. Rev. Stat. § 51:3074(A), et seq.;

q. Md. Code, Commercial Law § 14-3504(b), et seq.;

r. Mass. Gen. Laws Ch. 93H § 3(a), et seq.;

s. Mich. Comp. Laws § 445.72(a), et seq.;

t. Minn. Stat. § 325E.61(1)(a), et seq.;

u. Mont. Code § 30-14-1704(a), et seq.;

v. Neb. Rev. Stat. § 87-803(a), et seq.;

w. Nev. Rev. Stat. § 603A.220(1), et seq.;

x. N.H. Rev. Stat. § 359-C:20(1)(a), et seq.

y. N.J. Stat. § 56:8-163(a), et seq.;

z. N.C. Gen. Stat. § 75-65(a), et seq.;

aa. N.D. Cent. Code § 51-30-02, et seq.;

bb. Okla. Stat. Tit. 24 § 163(A), et seq.;

cc. Or. Rev. Stat. § 646A.604(1), et seq.;

dd. 73 Pa. Stat. and Cons. Stat. Ann.§ 2301 et seq.

ee. R.I. Gen. Laws § 11-49.3-4, et seq.;

ff. S.C. Code § 39-1-90(A), et seq.;

gg. Tenn. Code § 47-18-2107(b), et seq.;

hh. Tex. Bus. & Com. Code § 521.053(b), et seq.;

ii. Utah Code § 13-44-202(1), et seq.;

jj. Va. Code § 18.2-186.6(B), et seq.;

kk. Wash. Rev. Code § 19.255.010(1), et seq.;

ll. Wis. Stat. § 134.98(2), et seq.;

mm. Wyo. Stat. § 40-12-502(a), et seq.

138. Plaintiff and the Class seek all remedies available under their respective state data breach statutes.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class Against Defendant)

139. Plaintiff incorporates by reference and realleges each and every allegation set forth above, as though fully set forth herein.

140. Plaintiff bring this claim on behalf of himself and the Class.

141. The Declaratory Judgment Act, 28 U.S.C. § 2201, *et. seq*., authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes as applicable here.

142. Defendant owes duties of care to Plaintiff and Class Members, which require Defendant to adequately secure Plaintiff and the Class Member's PII.

143. Due to the Data Breach, Plaintiff and the Class Member's PII have been unnecessarily put at risk.

144. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff and the Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII.

145. Accordingly, Plaintiff and the Class request this Court under the Declaratory Judgment Act to enter a judgment declaring the following:

a. Defendant owes a legal duty to secure the PII of its former and current customers of Defendant;
b. Defendant has breached its duty to Plaintiff and the Class by allowing the Data Breach to occur;
c. Defendant continues to breach its legal duty by failing to employ reasonable means to secure the PII of Defendant's former and current customers.
d. Defendant's ongoing breaches of said duty continue to cause Plaintiff and the Class harm.

146. Plaintiff and the Class, therefore, seek a declaration that (1) each of Defendant's existing security measures do not comply with their obligations and duties of care to provide

reasonable security procedures and practices appropriate to the nature of the information to protect consumers' PII, and (2) to comply with their duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Engaging third-party security auditors and internal personnel to run automated security monitoring;
c. Auditing, testing, and training their security personnel regarding any new or modified procedures;
d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;
e. Conducting regular database scanning and security checks;
f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
g. Purchasing credit monitoring services for Plaintiff and Class Members for their respective lifetimes; and
h. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

147. The Court should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with the law and industry standards to protect Plaintiff and Class Members' PII.

148. If an injunction is not issued, Plaintifs and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant's systems or networks. The risk of another breach is real, immediate, and substantial.

149. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, Plaintiff and the Class will likely be subjected to fraud, identity theft, and other harms described herein. But, the

cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is minimal given it has pre-existing legal obligations to employ these measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, request judgment against Defendant and that the Court grant the following:

a. An Order certifying the Class, as defined herein, and appointing Plaintiff and their counsel to represent the Class;

b. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;

c. Injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. Requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff and Class Members' respective lifetimes;

iv. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the

Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

v. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. Prohibiting Defendant from maintaining Plaintiff and Class Members personally identifying information on a cloud-based database;

vii. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by third-party security auditors;

viii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. Requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

x. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;

xi. Requiring Defendant to conduct regular database scanning and securing checks;

xii. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class Members;

xiii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. Requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. Requiring Defendant to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

d. For an award of damages, including actual, statutory, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

e. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: January 26, 2023

BARRACK, RODOS & BACINE

/s/ *Andrew J. Heo*
Andrew J. Heo (N.J. Bar No. 296062019)
Jeffrey W. Golan*
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103
Tel: (215) 963-0600
Fax: (215) 963-0838
aheo@barrack.com
jgolan@barrack.com

/s/ John G. Emerson
John G. Emerson*
2500 Wilcrest Drive, Suite 300
Houston, TX 77042
Tel: (800) 551-8649
Fax: (501) 286-4659
jemerson@emersonfirm.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice applications forthcoming*